CLAIMS

We claim:

1. A method for manufacturing a trusted device comprising the steps of:

(a) receiving keying information from a manufacturer, said manufacturer having received said keying information from a licensing authority;

(b) generating a temporary private key;

(c) computing a final private key using said temporary private key and said keying information;

(d) computing a final public key using said temporary private key and said keying information;

(e) sending said final public key to said manufacturer for certification; and

(f) receiving a binding certificate from said manufacturer.

2. The method according to claim 1, wherein said keying information includes an initial private key and a device identifier.

3. The method according to claim 2, further including the step of forgetting the initial private key.

4. The method according to claim 1, further including the step of computing an evidentiary certificate.

5. The method according to claim 4, wherein said evidentiary certificate includes text and a signature of the text.

6. The method according to claim 4, further including the step of presenting a copy of said evidentiary certificate to a second device.

7. The method according to claim 4, further including the step of said second device verifying said evidentiary certificate.

8. The method according to claim 6, further including the steps of:

(a) said second device requesting a credential confirmation from said trusted device;

(b) said trusted device computing a credential confirmation; and

(c) said trusted device presenting a copy of said credential certificate to said second device.

9. The method according to claim 4, further including the step of presenting a copy of said evidentiary certificate to said licensing authority.

10. The method according to claim 4, further including the step of said licensing authority verifying said evidentiary certificate.

11. The method according to claim 10, wherein said step of said licensing authority verifying said evidentiary certificate further includes the steps of:

(a) recomputing the final public key from the keying information and the evidentiary certificate; and

(b) checking that the recomputed final public key with a manufacture's certificate.

12. The method according to claim 8, wherein said step of computing a credential confirmation includes using a hash function.

13. An apparatus for manufacturing trusted devices comprising:

(a) a licensing authority for providing keying information;

(b) a multitude of manufactures, each of said manufactures receiving keying information from the licensing authority; and

(c) a multitude of trusted devices, each of said trusted devices receiving keying information from one of said multitude of manufacturers and generating a final private trusted device key and final public trusted device key using the keying information;

wherein said manufacture certifies said public trusted devices key.

14. An apparatus according to claim 13, wherein said licensing authority includes a database, said database containing trusted device records.

15. An apparatus according to claim 14, wherein said trusted device records include a public key.

16. An apparatus according to claim 14, wherein said trusted device records include:

(a) a trusted device identifier; and

(b) a manufacturer identifier.

17. An apparatus according to claim 14, wherein said set top box records include a set top box public key.

18. An apparatus according to claim 14, wherein said trusted device records include a manufacturer certificate.

19. An apparatus according to claim 14, wherein said trusted device records include a communications identifier for identifying a device with which the trusted device may communicate.